RFID as a Tool in Cyber Warfare

RFID as a Tool in Cyber Warfare

Mikko Kiviharju
P.O.Box 10
FIN-11311 Riihimaki
FINLAND

mikko.kiviharju@mil.fi

ABSTRACT

Computer network operations (CNO) can have an effect technically over any systems using logical communications, not limited to nodes with Internet connectivity. We note in this article some more unconventional venues to attack information systems security with radio frequency identification (RFID) technologies, and develop a threat model for RFID in military use. Unprotected RFID tags offer a back door for adversaries even into closed systems, and without user interaction; on the other hand, rather simple RFID-solutions are placed to protect even very secure areas. The model includes two types of typical military applications for RFID: physical access control and logistics. The model discusses the process and framework for auditing existing systems and planning new establishments.

1 INTRODUCTION

Cyber warfare, especially computer network operations (CNO) have a deep technical aspect. Even minute technical shortcomings in the security of protected systems may lead to a complete compromise of the system. Conventionally, high levels of assurance have been achieved only with “six feet of air”, or physical (and electromagnetic) network separation. Lately, though, even this has not proven sufficient, as the case with `Agent.btz` – computer worm has demonstrated [6]. `Agent.btz`, sometimes even considered to be a real case of *military* computer network exploitation (CNE), used USB-flash memories to transfer malware into closed networks and leak data out of them.

Radio frequency identification (RFID) is rather a broad concept. In this paper, we refer to the architecture in fig. 1, where each of the components and communication protocols use widely known or standardized techniques to implement their functionality.

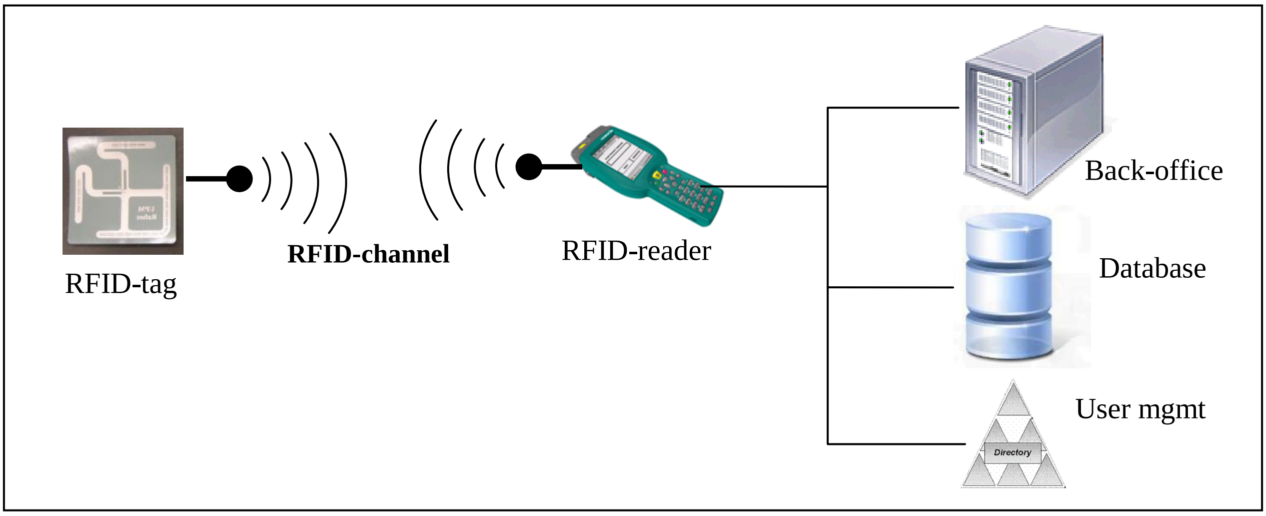

Figure 1: RFID system as a subsystem

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **NOV 2010**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**
4. TITLE AND SUBTITLE **RFID as a Tool in Cyber Warfare**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **P.O.Box 10 FIN-11311 Riihimaki FINLAND**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091

14. ABSTRACT

Computer network operations (CNO) can have an effect technically over any systems using logical communications, not limited to nodes with Internet connectivity. We note in this article some more unconventional venues to attack information systems security with radio frequency identification (RFID) technologies, and develop a threat model for RFID in military use. Unprotected RFID tags offer a back door for adversaries even into closed systems, and without user interaction; on the other hand, rather simple RFID-solutions are placed to protect even very secure areas. The model includes two types of typical military applications for RFID: physical access control and logistics. The model discusses the process and framework for auditing existing systems and planning new establishments.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**16**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

RFID technologies in general use the spectrum very broadly: systems vary from LF to UHF and microwave. Due to regulatory issues, the UHF-range solutions tend to have further read ranges than LF, reflecting in the applications area. The LF and HF systems are used for close-range applications, such as physical access control and payment systems. UHF, on the other hand, is typically used in logistics.

The RFID subsystem can be thought to be consisting of a tag, channel and a (possibly mobile) reader. RFID tags are categorized in three groups, based on their role in the communication protocol and energy use:

- Passive tags that don't have a battery on their own, but operate on the energy of the reader transmitted by the electromagnetic field
- Active tags that contain a power source, and can initiate communication based on that energy
- Semi-passive tags, which employ a power source for extending their read range and holding internal state, but do not initiate communication unsolicited

In our view, RFID technology represents a similar threat in CNO as USB sticks, only more insidious due to the following characteristics:

- RFID systems are often readily connected from the edge of the closed network right to the core
- RFID technology, when present, is an integral part of the setup, going unnoticed
- Processes involving RFID are optimized to require as little user interaction as possible
- Traditionally, RFID-subsystems are considered as trusted, requiring little or no security (relying mostly on the vendor's IPR protection, a.k.a. "security through obscurity")

Due to the low cost, small size and weather-resistant packaging of some RFID tags, it is possible, for example, to construct a cyber minefield, with different types of virus-infested tags, such that when enemy battle systems move over the minefield, their RFID readers will pick up the contamination and disable or corrupt some of the mission-critical systems. This is one way the short-range wireless sensor types could be used to penetrate the seemingly thick wall of physical network separation of operational systems, and deliver information warfare type operations into closed networks.

The purpose of this paper is to present the results of our work for identifying and tackling the RFID threat in the CNO framework.

2 SCENARIOS

In the course of our research, we have identified two of the most typical scenarios using RFID in the military: logistics and physical access control. The requirements of the scenarios for INFOSEC and COMSEC are elaborated below.

2.1 Logistics

In logistics, there is need to monitor items and vehicles (fleet management) automatically, when they are stored and transported between locations. Typical tracked properties are, for example, environmental conditions and location. Tags could be placed on several types of items, from large containers down to individual rifles.

For logistics, the availability and integrity of the information in a larger scope has more weight than e.g. the confidentiality of single tags. These properties contribute to the situational awareness in logistics as well as the functionality of the whole logistics chain. (If the container destination addresses are mixed in a specific holding area, it could severely delay or even destroy the logistics of an entire mission.)

It is characteristic in logistic systems to have deep-reaching connections from the RFID subsystem to the internal database servers. This presents an extra attack vector not often present in access control systems.

2.2 Access Control

RFID is replacing or augmenting physical locks in many places. The sometimes rapid changes in personnel and facilities force the physical access control systems to be very flexible. Mapping from the user set to a lock set needs to be many-to-many, easily maintained and quickly configured. Administration needs to be able to centrally assign and revoke rights per lock and per user or group of users. Restrictions can also be based on the time of day, person of facilities classification or special circumstances.

Physical access control has two concerns:

- Preventing unauthorized access into facilities
- Ensuring access for authorized users

Thus the systems need to guard the confidentiality of single user's private access information as well as ensure the availability of the service as a whole.

The central access control management systems are usually separated from other systems and networks, so the attack paths from the access control to other mission critical systems are lengthy and unlikely. Additionally, the access control tags need not contain much memory or processing logic, making the threat of malware in the tag less prominent.

3 THREAT MODEL

RFID systems have long been isolated and proprietary systems, mainly due to their size and processing restrictions. This position has been very tempting for the vendors to overlook costly information security issues: the related risk has not so far presented a substantial threat to critical systems. However, due to the increased connectivity of RFID subsystems, their threat potential has increased nearly exponentially.

In our scenarios, the approach taken by some of the vendors has resulted in two main threat vectors. The first one is introduced by the increased connectivity is considering the RFID subsystem as a weapon instead of a target. From an abstract point of view, the RFID subsystem may represent an unguarded route to critical core systems, even in cases where the critical system has been physically separated from other networks.

The second threat vector is the low entropy of the tags in the access control system tags, allowing a fast enumeration of all the possible key alternatives, much like having a master key to the locks of a whole facility.

In the following, we detail the threat model and its application to our scenarios. This includes the attacker presumed abilities and restrictions as well as different attack types with examples and effects.

3.1 Attacker Abilities

The attacker abilities are modelled based on two typical models: Dolev-Yao for the general computer network security [1], and Chosen Ciphertext Attack (CCA) for the cryptographic components [7]. We applied these models to the RFID subsystem.

Dolev-Yao: the attacker

- can read the RFID channel at sufficient rates; specifically the attacker can demodulate the code, decode the line coding and discover possible hopping sequences

- can write to the RFID-channel at sufficient rates
- can inject compromised or even customized tags and readers to the system
- can corrupt a limited set of legitimate readers and tags, but not
  - corrupt their private data (i.e. smart card crypto keys)
  - readers without the interaction of the reader with the RFID-channel
- can *not*, in the general case:
  - delete RFID-traffic from the RFID-channel, implying that removal or rerouting of messages in the RFID channel is deemed infeasible, and modifying messages requires moderate to large resources and expertise
  - decrypt logical level ciphers or predict random number generators' output

CCA: the attacker:

- can recover the encryption algorithm used, in detail
- can deceive the hardware and processes working under operative crypto keys to encrypt and decrypt arbitrary messages subject to the following constraint:
  - messages sent according to the pre-specified functionality of the system by legitimate and uncorrupted components can be encrypted and decrypted only case by case

Table 1: RFID threat categories

	Tag (T)	Channel (C)	Reader (R)
Confidentiality (C)	TC_READ	CC_SNIFF	RC_READ
	TC_META		
	TC_UNKILL		
Integrity (I)	TI_OVR_GEN	CI_INJ	RI_REPLACE
	TI_OVR_CODE	CI_MITM	
	TI_OVR_FUN		
	TI_CLONE		
Availability (A)	TA_KILL	CA_DOS	RA_DISABLE
	TA_RDR		
	TA_BLOCKER		

The threat model differs for access control and logistics cases for practical reasons: the logistics case is far more general, and requires a meta-level approach. It is possible to translate each model to the same type as the other, but in such a case the application will be more laborious. As the logistics case has a more general model, we recommend using that one for cases outside their domain.

3.2 Logistics

The logistics threat model considers all three types of attacks in the CIA-model (confidentiality, integrity and availability) targeted against each of the RFID-subsystem components: tag, channel and reader. These

are then translated into examples and effects in the logistic and access control environment, displayed in table 1 and explained in tables 2-4.

It should be noted that the focus is on attacks to the tag and channel, as these are easiest for the attacker to get access to; in addition, the compromise of components further up the chain towards the backend systems nearly always implies the compromise of the components "below". Thus attacks targeting the reader from the back office are not considered, and attacks channelling from tag or the channel are grouped under respective categories.

Table 2: RFID tag-based threats and their effect in logistics

	Code	Explanation / example	Effect (in logistics)
Conf.	**TC_READ**	Unauthorized reading of tags; the possibly sensitive information in a tag or a their combination in a group of tags is leaked	Force tracking; deduction of operations by e.g. rifle IDs
	TC_META	Unauthorized deduction of metadata from the tag information (e.g. batallion ID, destination, PIN-code)	Intelligence on the blue force movements and hierarchy are leaked
	TC_UNKILL	Restoring information in a "destroyed" tag	"Dumpster diving", i.e. accessing sensitive information thought to be safely discarded (encryption keys, etc.)
Integr.	**TI_OVR_GEN**	Unauthorized overwriting of tags: tags contain inaccurate or false information	Items are transported to incorrect destinations, the logistic situational awareness is distorted
	TI_OVR_CODE	Tags contain malware affecting the backend systems, such as viruses or backdoors.	Takeover of the back office or user management systems, injecting viruses into the main systems
	TI_OVR_FUN	Changing the operational logic of the tags (injecting unauthorized commands to tags)	The tag will send continuously, ending the battery; tags will refuse to answer to authorized requests, but answer to unauthorized ones (i.e. track their location and send it to the attacker whenever possible)
	TI_CLONE	Breaking the connection between the tag information and the physical, authorized token represented by the tag (cloning or destroying the tag)	The basis for the identification is broken; distortion of the situational awareness of logistics ("ammunition left: 100 boxes", when in fact very few are left)
Avail.	**TA_KILL**	Disabling the tags nearly permanently (e.g. a "kill"-command)	Items are misplaced and their transport slowed down; situational awareness in logistics updates slowly or is distorted
	TA_RDR	Using a contaminated tag to crash the reader applications or operating system	Slight distortion in the situational awareness in logistics
	TA_BLOCKER	Disabling the tags by actively blocking their radio channel or communication protocol	cf. TA_KILL; more easily remedied

Table 3: RFID channel-based threats and their effect in logistics

	Code	Explanation / example	Effect (in logistics)
Conf.	CC_SNIFF	Eavesdropping	cf. TC_READ and TC_META
Integr.	CI_INJ	Injecting unauthorized messages in the channel; breaking the authentication of the channel	cf. TI_OVR_* and TC_*
	CI_MITM	Man-in-the-Middle attack (rerouting a message, altering a message actively during a protocol run)	Slight distortion in the situational awareness in logistics
Avail.	CA_DOS	Blocking the communication channel with other than electronic warfare methods, i.e. RFID-DoS attacks (e.g. an unauthorized reader can query tag information too rapidly; a set of unauthorized tags can send hello-messages faster than standardized)	cf. TA_KILL

Table 4: RFID reader-based threats and their effect in logistics

	Code	Explanation / example	Effect (in logistics)
Conf.	RC_READ	Unauthorized reading of tag contents from the reader; the possibly sensitive information in a tag or a their combination in a group of tags is leaked	cf. TC_READ and TC_META
Integr.	RI_REPLACE	Replacing a trusted reader with an unauthorized reader	All the tag- and channel-based threats
Avail.	RA_DISABLE	Disabling or destroying an authorized reader by another means than via the RFID-channel (i.e. physically)	cf. TA_KILL, TA_RDR, TA_BLOCKER and CA_DOS

Not all of the threats are equally significant. The significance of the threats forms an application-specific RFID threat profile, which we have categorized as follows:

- *Critical*: system cannot be accredited / operation of existing systems should be discontinued
- *Major*: the threat should be handled according to the risk management policy as soon as possible
- *Prioritized*: the threat should be handled according to the risk management policy
- *Minor*: the threat should be acknowledged on a per-system basis

For logistics, the RFID tags are not usually placed very individually (per soldier) but attached to more collective units, such as containers. Thus, hostile force tracking is not as likely. In addition, the situational awareness picture is formed as a total from a large set of widely distributed tags, making a local breach less significant.

On the other hand, certain computer virus types have been demonstrated to fit into as low as 100 – 200 bytes [5]. This can easily be accommodated in the storage capacity of most modern RFID tags – even EPC

Global Gen2 standard passive tags include a maximum of 88 bytes of memory [3], well within the reach of skilfully optimized virus codes. As the RFID subsystem is very often optimized in cost, the tag memory content is simply passed along the route – without validation - to the core systems, which finally consumes the unfiltered payload. As the logistic IT-systems are well networked into the core operational C2 systems, this poses a significant threat for the back-end systems *via* the RFID.

In the logistics application, RFID can be transformed from an enabler to a cyber warfare tool. Otherwise closed C2 systems may have unexpected unguarded routes past their security perimeter, leading to both information leakage and internal information corruption. The detailed RFID threat profile for logistics is, according to our studies, as follows:

- *Critical*: TI_OVR_CODE, CI_INJ, RI_REPLACE
- *Major*: TI_OVR_GEN, TA_KILL, RA_DISABLE, TA_RDR
- *Prioritized*: TI_OVR_FUN, TA_BLOCKER, TC_META, TC_READ, CC_SNIFF, RC_READ
- *Minor*: TI_CLONE, CI_MITM, CA_DOS

3.3 Access Control

The access control threat model stems from the more precisely defined subsystem, including personal tags and possible PIN-codes, reader functionality (opening a door and relaying / checking a PIN) and placement (at entrances and security perimeters), and back-end functionality (user- and group management, auditing). We were able to pinpoint the threats in a more practical level, and map the dependencies between each threat. The work was performed jointly with Oulu University Secure Programming Group (OUSPG) and the framework has been published separately in [8].

In current access control systems much of the security is often implemented with “security by obscurity”. Thus, for existing systems, even reverse engineering can be considered a security threat. Certain issues related to privacy in conventional systems can also be seen as a threat in access control systems: for example marking the tags (which act as security tokens) too clearly with their intended purpose may help the attacker to select its targets better.

We present here only a summary of the detailed threats identified in [8], but describe here instead the RFID threat profile for access control translated into the general threats specified in the logistics section.

Table 5: RFID threat-vectors in access control

Threat	C?	I?	A?	Arch. elements
BackendFloodingThreat			**X**	Backend
BadHashThreat	**X**	**X**		All
BadPrngThreat	**X**	**X**		Tag, Reader
BruteForceKeySpaceThreat	**X**	**X**		Tag
DeltaDebuggingPacketThreat	**X**			All
DeltaDebuggingThreat		**X**		Channel
DenialOfRfChannelThreat			**X**	Channel
DenialOfServiceThreat			**X**	General
DenialUsingAnticollisionThreat			**X**	Channel
DisconnectionThreat		**X**	**X**	Reader, Backend
ForgeryThreat		**X**		Tag, Backend
GetPinFromTagThreat	**X**	**X**		Tag
GetPinFromUserThreat	**X**			Reader
KeyCopyingThreat	**X**	**X**		Tag
KeyLeakingThreat	**X**	**X**		All
PoorlyUsedKeySpaceThreat	**X**	**X**		Tag
ReaderBreakingThreat			**X**	Reader
ReaderTracingThreat	**X**			Reader
RelayingThreat	**X**	**X**		Channel
ReplayThreat		**X**		Channel
RfidDataMalwareThreat	**X**	**X**	**X**	General
SpecLeakingThreat	**X**	**X**		General
TagbreakingThreat			**X**	Tag
TagCollisionIdTrackingThreat	**X**			Tag
TagHolderRecognitionThreat	**X**			Tag
TagReaderRecognitionThreat	**X**			Reader
TagSignalFingerprintTrackingThreat	**X**			Tag
TagTrackingThreat	**X**			Tag
UnauthorizedAccessThreat	**X**	**X**		General
WeakBackendHashThreat	**X**	**X**	**X**	Backend
WeakEncryptionThreat	**X**	**X**		General

In cyber warfare, a significant part of hacker attack preparation is intruding some of the premises containing network operations equipment, such as NOCs (Network Operation Centre). If these premises are physically protected with RFID access control technology, its threat profile poses an equally large risk for the mission critical systems as planting malware.

The RFID threat profile for access control was identified as follows:

- *Critical*: TI_OVR_CODE, TI_CLONE, TC_READ, RI_REPLACE, RC_READ
- *Major*: TA_KILL, CA_DOS, TA_RDR, CI_INJ, CC_SNIFF, CI_MITM, RA_DISABLE, TC_META
- *Prioritized*: TA_BLOCKER
- *Minor*: TI_OVR_GEN, TI_OVR_FUN

4 AUDITING

The acquisition of third-party commercial hardware and software for military purposes is becoming increasingly commonplace. Ideally, sufficient and authenticated information of the acquired system can be readily accessible for the system users, and the claimed functionality corresponds to the actual real-life functionality. However, too often the relevant security properties are too vaguely specified and / or inadequately implemented in the system. Auditing is required to validate that the claimed security properties of system are present.

Technical security audits for conventional ICT systems have well established procedures for varying degrees of depth (e.g. [2]. However, due to the nature of RFID systems, there is considerable significance on the reverse engineering process, or establishing the inner workings of the system. This nature stems from

- Wide variety of technologies and vendors within the RFID subsystem, from radio technology to logistics applications
- Extremely optimized manufacturing processes to produce cheap tags and readers, leaving little motivation for the vendor to disclose the more detailed functionality of the RFID-components, making the available documents rather vague about the security properties of the system
- Tendency to rely on “security by obscurity”, i.e. omission of security measures in the hope that if the details remain secret, the system cannot be fruitfully attacked

The RFID security auditing process follows the main principles in typical information system audits [2,9], that is:

- Planning and preparation
- Performing risk analysis based on a threat model and the goals
- Gathering necessary information about the audit target
- Analyzing the gathered information based on the threat model and the claimed functionality
- Disclosure of the results

The process for the audit is similar for both of our applications: access control and logistics. However, the required tools for analysis and information gathering vary somewhat, mostly depending on the RFID channel characteristics and reader platform.

4.1 Process

The general process is depicted in figure 2. The process is iterative in nature, as some later details may reveal new threats or vulnerabilities not anticipated beforehand, and requiring explicit permissions from management and vendors. (The exception to this is the results disclosure, which needs to be kept a separate process. If new important vulnerability information comes up during this phase, a new audit process may need to be started.) We anticipate at least two iterations, as the audit targets need to be refined at least once.

Planning and preparation includes the audit target identification, initially at a coarse level, but refining them during the process. Purpose statement includes a clear indication of the audit’s expected results, motivation, and scope, e.g.

- Examination of a product against vendors claims and domestic security policy
- Audit of an internal system against a new security policy

- Checking a product implementation against its specifications
- Checking compatibility of a certain department IT systems with respect to a new legislation or standard

An obvious, but not to be underestimated, part is the management buy-in: especially external audits may be sensitive topics, and not possible to conduct with low-level acceptance only. Generally, the RFID setup may require actions (such as reverse engineering) that need vendor permissions / support. This is, however, dependent on local legislation and audit depth.

Risk analysis does not require the auditor to identify the assets and their value, but rather obligates the audit target owner to provide sufficient information to the auditor. The general risk analysis is then viewed with the RFID-specific threat model (e.g. the one presented before), identifying, for example:

- Which of the critical assets are theoretically accessible from the RFID subsystem
- What kind of attackers might be likely to access the assets and what resources are they likely to spend on it (in terms of hardware, knowledge, skills and inside information)
- Which of the threats listed in the threat model can be afforded by the attacker in consideration (based on the resources needed for the attack)?

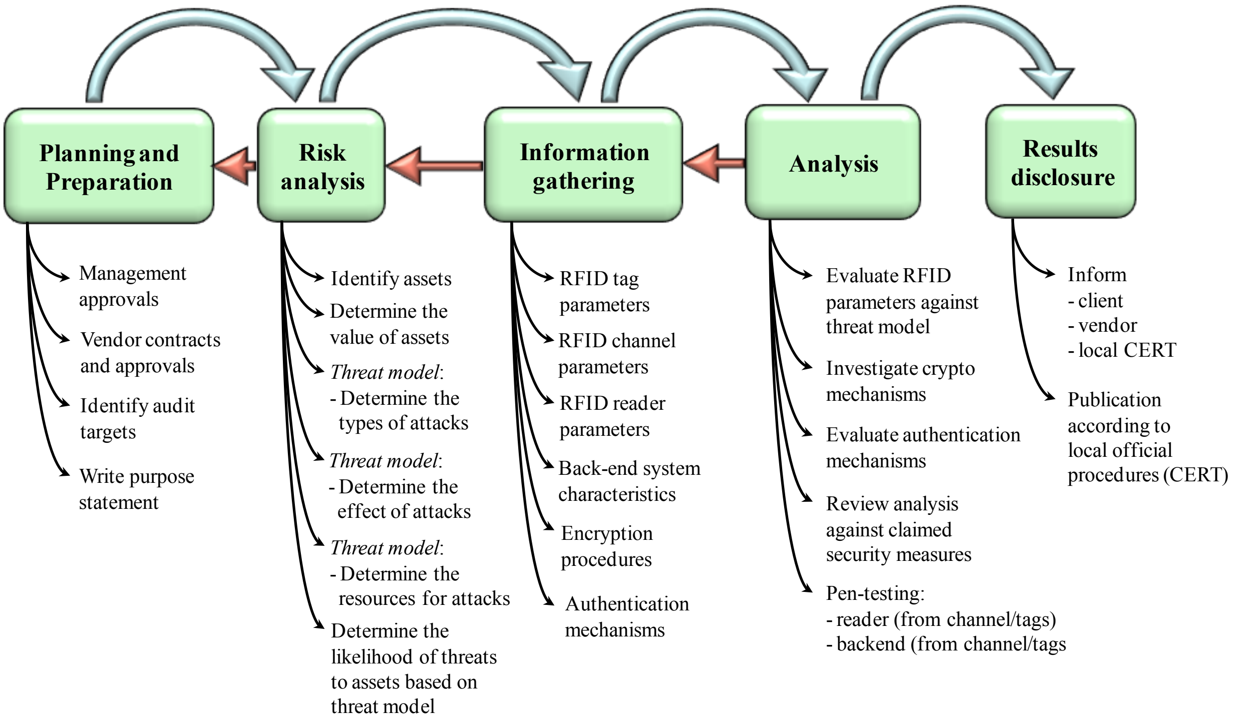

Figure 2: RFID security audit general process

Information gathering is, by our experience, the most laborious part of the audit. This is especially true with the access control case, as the systems are closed and small-scale, acquired from a large multi-national vendor via a chain of resellers and system integrators.

An audit, whose purpose is to harden systems against CNO, needs to investigate protocols, encryption schemes and other security controls on a logical level. However, for closed systems, this requires accessing the information on the physical level as well, not to mention knowledge on the data encoding, protocol type, data formats, etc.

If the system proclaims to follow a known standard, the information gathering phase is made easier by an order of magnitude. In most cases in logistics, this seems to be the case, but the access control systems often follow vendor-specific, and sometimes old conventions on defining the operation and formats of the RFID subsystem. We divided the information into six:

- RFID tag parameters, such as data encoding and format, memory size and usage (including security controls), accepted command language (if any), tag type and population control response
- RFID channel parameters, such as frequency, modulation, symbol speed and data encoding
- RFID reader parameters, such as data encoding and format, memory size and usage, accepted command languages, supported tag and population control types, external communication interfaces and their protocols, typical operation with the tags
- Back-end system characteristics: system type (database, ERP-software, user management, ...), security controls for the channel including data input from the RFID subsystem
- Authentication mechanisms and protocols, between the tag and the reader, and the reader and the back-end system
- Encryption methods: cryptographic algorithms, hash algorithms, pseudo random number generators (PRNG) and key management (including tokens and PIN-codes)

The analysis part here includes the actual review as well. Note that after information gathering it is likely needed to step back to refine the planning and preparation as well as the risk analysis. The review is meant to compare the results of the information gathering with the specifications and claims, which in turn are compared to the original contracts, security policies and / or standards and legislation.

Actual analysis is likely to be required on the different security controls in the RFID-subsystem, such as key management, PRNGs, use of cryptographic modes, protocols and authentication mechanisms, whether they actually fulfil their intended purpose.

Penetration testing is recommended in two cases:

- If the RFID reader blackout is sufficiently serious for the operation
- If the RFID reader transmits large enough packets (> 50B) of data to the back-end systems to give rise to malware injection attacks against the back-end systems

An alternative to pen-testing is to have sufficiently detailed documentation of the security controls in the RFID-reader (basically indicating a source-code audit).

Results disclosure finalizes the audit process. Note that due to the nature of a standard vulnerability disclosure process, it is generally very difficult to iterate backwards from this stage. The disclosure process may follow the standard conventions for RFID as well, noting again the possible discrepancy between the size of the vendors and the typical user organization.

4.2 Tools

We focus here on the tools required especially for the RFID auditing process. Tools for formal protocol analysis and pen-testing are available elsewhere, and can be used independently of the RFID subsystem. We did not consider the more advanced attacks, such as reprogramming a reader, but concentrated on attacks originating from the RFID-channel. This is due to the following reasons:

- It is possible to simulate any tag or reader operation to the other party by manipulating the channel only.
- If the tag is modifiable from the reader, new and customized tags can be generated (to a degree) from injecting suitable message in the channel only.

RFID-channel manipulation needs physical devices to send and receive data. Due to the multiple frequencies used in different RFID systems, different radios may be required. Based on our experience, LF and HF can be managed with the same radio and several antennas, but UHF and microwave bands require separate radios, even within UHF (e.g. ISO-18000-6c and 18000-7 systems are best analyzed with different radios).

UHF-radios are usually specialized systems due to the large symbol speeds compared to current state-of-the-art in general purpose computing platforms. For LF and HF systems, low-cost open hardware platforms exist (e.g. GNU-radio [4]).

The heart of the radios is naturally operating systems and signal generation software. Additionally, signal analysis tools are needed. We developed in conjunction with OUSPG a set of signal analysis and radio controller tools, available in [8]. These include:

- Different modulation generation and recording tools for the GNU-radio
- Demodulation tools
- Signal analysis tools
- Transmitting tools
- Data format manipulation tools
- Syntax analysis tools
- Automatic data generation tools
- Reference signals

The tools were tested only for the LF and HF signals. For UHF signals, a different set was developed.

5 CASE STUDIES

The audit process and tools were developed with the help of case studies, one from each of the application areas. The logistics case study involved a UHF active tag system used for item tracking, and the access control case a passive tag system for electronic door locks.

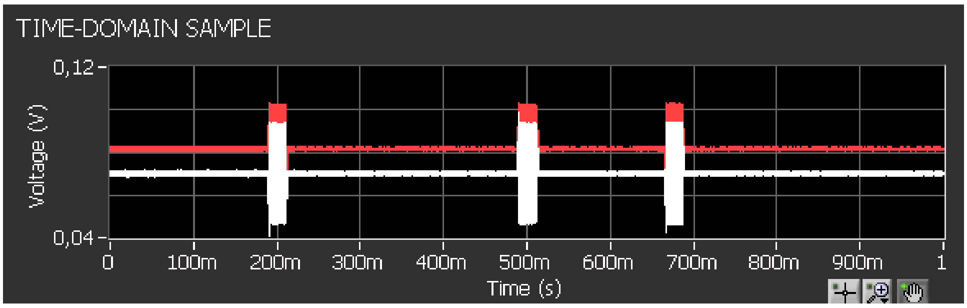

Figure 3: Data bursts and their spectrum of the active tags, indicating 2-FSK

5.1 Logistics

The active tag system investigated was built on a US-based company chip technology, repackaged and programmed by a Finnish company for fleet management. The tags were placed in containers, were they measured different environmental conditions as well as location. The system consisted of the tags, which transmitted about 30-100 meters regularly trying to contact a reader within range. When a reader appeared within range, the tags dumped their measurement information to the reader, which forwarded them over its WAN-connection to a centralized database.

The system was in an evaluation phase, and the purpose of the security audit was to find possible technical weaknesses in the RFID-subsystem. The audit was requested by the potential acquiring organization, and since the system was in evaluation phase, the Finnish reseller was co-operative in providing the sufficient information. However, some of the RFID channel characteristics were tied to the tag's chip itself, making it necessary to verify the Finnish reseller information separately.

We used the threat model described in chapter 3.2. For the information gathering phase we used a separate signal analyzer (different from the tools depicted in [8], due to the symbol speed, which the standard GNU-radio communication circuits could not handle adequately), dedicated for 800 – 1000 MHz band. The modulation recognition required yet more equipment (it turned out to be a form of FSK – RFID systems do not deploy complex modulation types, thus making them easy to identify; see fig. 3).

During information gathering and subsequent analysis, the main weaknesses found in the system were as listed below:

- No explicit authentication between the tag and the reader, beyond a shared secret key used in the communication encryption
- Communication in the RFID channel was encrypted, but the encryption keys were kept constant, and the encryption mode was that of a stream cipher. Thus XORing a known plaintext and the sniffed ciphertext, one could recover the keystream easily.

- Together these two weaknesses enabled a total control of the RFID channel by an attacker
- The reader was forwarding the measurement data without sanitation to a database management server, which inserted the data also without sanitation directly into the database.
- The packets forwarded by the reader could be between 100 and 200 bytes, making it large enough to contain viruses or SQL-injections
- The latter two weaknesses enable an attacker to inject malware from the tags right into the core systems, or to take full control of the database using an SQL injection.

Based on the analysis, the system could not be recommended for deployment, unless the weaknesses were resolved. (Later, however, the whole technology type was discarded due to compatibility issues).

5.2 Access Control

All of the access control RFID-subsystem's technology in our case is developed and marketed by a large multinational corporation. The integration into an access control and workforce tracking software was made by a Nordic integrator. The RFID subsystem in question has been broken multiple times in the past, but the vendor has prevented large scale publication through litigation, allowing the weaknesses to remain in place. Due to the closed nature of the product, as well as little or no available exact information on the weaknesses, the system was considered viable for a security audit by the organization employing it as their access control method.

The system consists of a passive LF tag, read normally from a distance of a few centimetres, and checked against access rights in a centralized server. It is possible to install a separate keypad beside the lock to require a PIN code as well as presentation of the token. The backend system is used to define the rights, as well as manage the key populations.

Since even the Nordic integrator would not provide or did not have the specifications of the system, it was reverse engineered from the physical layer upwards. As the system works in the LF band, it is possible to use generalized radio equipment and standard laptops for analysis and signal generation. (See [8] for a more detailed description of the auditing system.)

We used the threat model described in chapter 3.3. Modulation recognition was trivial, since the ASK modulation shows up in a basic oscillator screen. The system did not contain enough information capacity for malware to reside in the tags, but neither was it sufficient to enforce any rigorous access control. The main weaknesses were:

- The identification was based on the static contents of the tag only, making it possible to clone the tag
- The tag variable, personally identifying, information content was only 12 bits, after facility code was known. This 12-bit "ID-space" was not used equally, but in large clusters (a set of keys ordered in the same patch were sequentially numbered). This enabled brute-forcing the entire keyspace, even without knowledge of any key.
- The PIN-code was not independent of the key-ID, instead it was computed from the ID using a deterministic algorithm (thus could not be changed, if revealed).
- If the reader connection to the backend system was disconnected, they checked only the facility code, not the individual code nor its access rights.
- These properties lead to an attack, where even a PIN-protected door, where only one key in the whole facility had rights to, could be brute-forced open in less than an hour (in seconds, if it was not PIN-protected).

Based on the analysis, the access control system was completely inadequate. The audit recommended replacing the system, which the organization put immediately under process.

Because of the vendor's history with vulnerability disclosures, the audit team left the disclosure process to be handled by the Finnish CERT-group. We are not aware of the process status, as of the time of writing this paper.

6 CONCLUSION

We have presented a threat model and an security auditing framework for an RFID-subsystem in military scenarios. Based on the threat models and our case-studies we have shown that RFID technology can be used in CNO both as a courier for malware over network separation and to breach physical access control systems.

Because of the multiple applications and ease of use, RFID technologies will continue to increase in popularity and appear in ever more unexpected places, even in military systems. Despite its current shortcomings in the information assurance arena we believe that RFID can be safely and securely integrated into other ICT systems. It *is* paramount to exercise care and perform similar validations for RFID systems as with any other new ICT system, but the security problems so far do not preclude the use of the whole RFID technology.

RFID should be included, with other ICT systems, early into company and organization risk analysis, and exercise similar caution and validation processes with RFID as with any other ICT system waiting for deployment. The bottom line is not to treat RFID subsystems as trusted, and not to assume physical separation will provide absolute protection from CNO.

7 REFERENCES

[1] D.Dolev, A. Yao. *On the security of public key protocols*, Proc. of the IEEE 22nd Annual Symposium on Foundations of Computer Science, pp. 350-357, 1981.

[2] ISACA. *IT Standards, Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals*, Information Systems Audit and Control Association, available at: http://www.isaca.org/AMTemplate.cfm?Section=Standards2&Template=/ContentManagement/ContentDisplay.cfm&ContentID=55920 1.3.2010.

[3] ISO/IEC. *International standard ISO/IEC-18000-6, Information Technology, Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz, Amendment 1: Extension with Type C and updates of Type A and B*, 15.6.2006.

[4] J.Lang. *GNU Radio*, in: http://gnuradio.org/redmine/projects/activity/gnuradio, 15.3.2010.

[5] M.Rieback,. B.Crispo, A.Tanenbaum. *Is Your Cat Infected with a Computer Virus?* Proc. of the 4th IEEE conference on Pervasive Computing and Communications, pp. 169 – 179, IEEE Computer Society, 2006.

[6] S.Shevchenko. *Agent.btz – A Threat That Hit Pentagon*, in: http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html, (Threat Expert weblog) 30.11.2008.

[7] D.Stinson. *Cryptography, Theory and Practice*, §1.2., CRC Press, 1995.

[8] University of Oulu. *FRONTIER-RIDAC - An Open Source RFID Audit Framework*, in https://www.ee.oulu.fi/research/ouspg/RIDAC, 1.3.2010.

[9] Wikimedia Foundation. *Information Security Audit*, in: http://en.wikipedia.org/wiki/Information_security_audit, 23.2.2010.